Written evidence submitted by WebGroup Czech Republic, a.s. and NKL Associates s.r.o.

Written Evidence to the DCMS Sub-Committee on Online Harms and Disinformation
Submitted by WebGroup Czech Republic, a.s. and NKL Associates s.r.o.

I. INTRODUCTION

1. WebGroup Czech Republic, a.s. (formerly WGCZ s.r.o.) and NKL Associates s.r.o., which specialize in the online hosting of adult content and own the websites xvideos.com and xnxx.com, respectively, (collectively "**WGCZ**" **or** "**we**") welcome the opportunity to submit this written contribution to the DCMS Sub-Committee on Online Harms and Disinformation (the "**Committee**") on the UK Government's Draft Online Safety Bill published on 12 May 2021 (the "**Bill**").

2. In the first instance, we are, respectfully, cognisant that it is, on its face, unusual for companies established in the Czech Republic to take an interest in a regulatory development in the UK, given that the UK is no longer part of the European Union and subject to the European *ordre public*. However, as the Committee will appreciate, the borderless nature of the Internet means that this proposed legislation has the potential of having ramifications beyond British borders; indeed, the Bill has the potential of affecting not only WGCZ, but businesses in all corners of the world.

3. WGCZ are operators of online platforms which host adult material, targeting an adult audience. WGCZ fully supports the goals of ensuring the health, safety and well-being of children online, including, among other things, by denouncing children's access to any content or product that is addressed to an adult audience. WGCZ underlines that it has never targeted any such audience and does not condone any such access and concurs on the importance of finding effective ways to prevent it. WGCZ has over the years collaborated with authorities all around the globe to join forces in the fight against child sexual exploitation and abuse (**CSEA**) content and to facilitate online child protection. WGCZ is fully cognisant that designing robust and proportionate interventions to protect children from accessing adult content without limiting adult access to the internet presents a policy conundrum.

4. Our submission is therefore intended, in the spirit of supporting initiatives to prevent minors accessing adult services, to provide the Committee with an appreciation of the impact of this legislation and to invite it to carefully scrutinise the proposed framework. While there is no doubt the Bill's aims of promoting safety online is commendable, it is not without challenges in a globally interconnected system. It is in the interests of both businesses and policy makers that its proposed solutions are effective, balanced, and appropriately accommodate the interests of the many users who use and rely on the Internet.

5. We note that the current Bill has expanded its remit to expect providers to be able to manage *any* potential harm that occurs on their platforms. There are some good intentions here – there is no harm in providers demonstrating their risk assessments in considering how they support the "safety" of users and providing a level of accountability for those less scrupulous providers who do not see the wellbeing of their platform users as their concern. However, as noted in section II below, the concept of the 'duty of care' is amorphous and the Bill fails to set out the extent of a duty of care that providers may have, and what the limits on expectations of protection should be.

II. THE INHERENT LIMITATIONS OF TECHNOLOGY

6. While no one can doubt the policy objective of protecting underage access, the proposal does not address or resolve the core of the challenge: the delicate balance between the importance of the objective and the intrusiveness, in terms of civil liberties, of truly effective measures to prevent underage access.

7. In making this submission, we are mindful of the fact that the Online Safety Bill follows a suite of successes (filtering on public WIFI which in itself is a highly contentious issue), near misses (default filtering on home ISP connections, still only used by a minority of households according to OFCOM[1]), and failures (Part 3 of the Digital Economy Act 2017). As this submission seeks to explain, the reality is that the Bill is not laid on a foundation of success in technology regulation or the use of technology to manage online behaviour.

8. Online services, and the underlying technology that allows them to be implemented, are global by nature. Therefore, geographical boundaries present problems. However, to try to isolate based upon geography is a challenge that introduces extraterritorial jurisdictional issues that are evident within this bill. Geography in an online sense is usually managed through the IP address system, where different countries are assigned different address ranges which, in turn, allows systems to make an approximation of the location of an end user. However, this is not a perfect system and work arounds such as IP proxying and Virtual Private Networks, which are widely used for many privacy enhancing measures, will easily circumvent this. Therefore, any legislation that attempts to control a global system from a geographically restricted perspective is not going to be perfect.

III. ADDRESSING ONLINE HARMS: THE TANGIBILITY AND PRACTICAL WORKABILITY OF THE "DUTY OF CARE" CONCEPT

9. The Bill's most significant innovation is the establishment of a "duty of care" on service providers, which includes duties to address illegal CSEA content.

10. In that respect, the Bill proposes to impose a number of "duties" on user-to-user service providers. Taking the example of "safety duties", the Bill provides:

---

[1] https://www.ofcom.org.uk/__data/assets/pdf_file/0025/217825/children-and-parents-media-use-and-attitudes-report-2020-21.pdf

"*(2) A duty, in relation to a service, to take proportionate steps to mitigate and effectively manage the risks of harm to individuals, as identified in the most recent illegal content risk assessment of the service.*

(3) A duty to operate a service using proportionate systems and processes designed to—

(a) minimise the presence of priority illegal content;

(b) minimise the length of time for which priority illegal content is present;

(c) minimise the dissemination of priority illegal content;

(d) where the provider is alerted by a person to the presence of any illegal content, or becomes aware of it in any other way, swiftly take down such content[2]

11. The Bill also specifies that:

(6) In determining whether a step, system or process is proportionate for the purposes of this section, the following must be taken into account—

(a) all the findings of the most recent illegal content risk assessment (including as to levels of risk and as to nature, and severity, of potential harm to individuals), and

(b) the size and capacity of the provider of a service.[3]

12. As presently drafted, the duties introduced by the Bill are amorphous: it is difficult to assess what might be considered to be an "effective" versus "ineffective" way to manage the risks of harm to individuals, for example, or to understand what "systems or process" would be considered appropriate.

13. WGCZ would welcome clear guidance as to what the 'duty of care' entails. WGCZ, for instance, already adopts a robust system of content control which is aimed at eliminating any content that violates the integrity of minors and the reporting of such offences to competent police authorities, as specified in the websites' content control policies.

IV. THE DIFFICULTIES WITH PREVIOUS AGE VERIFICATION PROPOSALS

14. One of the possible "system or process" that have been previously considered is an "age verification mechanism", which this Committee will be familiar with as part of its past consideration of the Digital Economy Act.

---

[2] Clause 9(2) and 9(3) of the Bill

[3] Clause 9(6) of the Bill

15. The Committee will recall that during the consideration of the Digital Economy Act, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression wrote an open letter to the British government expressing his concerns about a number of the proposals:

> "*First, I am concerned that the age verification provisions* ***give the government access to information about citizens' viewing habits and data***. [...] *In addition, the age verification requirement can easily be abused, such as* ***hacking***, ***blackmail*** *and other potential credit card* ***fraud***. [...]
>
> *I am concerned about the lack of* ***privacy*** *obligations in the bill, when it effectively provides for the use of technologies that limit privacy rights through the requirement of age verification.* [...]
>
> *In addition, I am concerned about the lack of* ***judicial review*** *of the age verification regulator's authority to shut down websites that do not comply with the age verification requirement...*"[4] (emphasis added).

16. The Government's appointment of the British Board of Film Classification as the intended age verification regulator and its attempts to propose an 'age verification certificate standard' was also widely criticized by organisations such as the Open Rights Group, who wrote that the standard was "*pointless, misleading and potentially dangerous."*[5]

17. The Committee will also be cognisant that from a technical standpoint, any such age verification mechanisms could only apply within the UK, allowing users to access adult sites via VPNs or IP proxying, by simulating access from another jurisdiction where it would not be restricted.

18. Moreover, the imposition of such measures could also result in the unwarranted effect of pushing children towards the dark web, which is far more likely to provide access to illegal content (such as CSEA content). Given the nature of the content in these spaces, they attract many with a sexual interest in children, so driving young people to these spaces could be extremely dangerous for them. There is also the risk of increasing the sharing of pornography through peer to peer channels without the content moderation that is achieved on mainstream pornography channels, where no CSEA is permitted. Finally, these spaces will place young people at greater risk for arrest if they are being monitored.

19. Without a uniform, consistent, and free, age ID scheme, a technical solution will always struggle. So a provider might implement an age verification solution that uses a number of different measures (for example, the NSPCC/IWF Report/Remove service[6] uses

---

[4] Communication to the Government of the United Kingdom from the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (OL GBR 1/2017), 9 January 2017.

[5] Open Rights Group, 'ORG Report: BBFC Age Verification Standard is Pointless, Misleading and Potentially Dangerous', 14 June 2019, accessed at: https://www.openrightsgroup.org/press-releases/org-report-bbfc-age-verification-standard-is-pointless-misleading-and-potentially-dangerous/

[6] https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/remove-nude-image-

passport, driving licence or YOTI) but these will not be effective for all young people. To continue with the NSPCC/IWF service as an example, all of the AV measures used on that system have an associated cost. This will mean that many young people will not be able to afford to verify their age, and will not be able to use it.

20. It would seem unfair and unrealistic to expect companies to invest in risk assessment and subsequent software tools to implement risk mitigation measures, just to be told they will still be fined as they failed in their duty of care to let in a determined, duplicitous young person who decides to bypass age verification measures with either their parent's login or a Virtual Private Network.

21. We believe therefore that the Bill's proposal to formally delete the age verification mechanisms introduced by the Digital Economy Act 2017 is warranted, given the clear, demonstrated unworkability of those proposals.

22. If the Government is serious in its view the age verification has to be part of the online safeguarding toolkit, and placing expectations on companies to implement a foolproof system, they should propose the underpinning infrastructure, which is a national ID card scheme, and weigh all of the privacy concerns and debates that brings from the public.

V. PUBLIC AWARENESS AND EDUCATION ON ONLINE SAFETY

23. The Bill will not succeed without a parallel emphasis on developing public discourse and educating the public about safety online.

24. Children are increasingly adept at using new technologies and navigating the Internet. Parents must play the most crucial role in ensuring their children are adequately protected at home, for instance, using built-in and other widely available (and free) controls on content or filtering.

25. Measures should also be integrated in curricula and public education to increase online literacy and warn children of the risks and dangers of operating online, thereby enabling them to make rational and informed choices as they navigate the Internet and to adopt appropriate strategies when encountering troublesome content.

VI. CONCLUSION

26. WGZC reiterates its support for initiatives to prevent minors accessing adult services and, in particular, ensuring that well-meaning initiatives do not result in deleterious consequences such as forcing minors onto the dark web and other more dangerous parts of the internet. We thank the Committee for the opportunity to provide our written observations on the Government's proposals in the Online Safety Bill and welcome the possibility of further engagement with the Committee and its members as the Bill goes through the parliamentary process.

---

shared-online/

27. As a responsible business, we must and do comply with laws and regulations, and in the present case, we respectfully ask the Committee to consider the importance of ensuring that the final legislative framework adopted by Parliament and which will become law protects fundamental rights, including the most cherished rights of privacy and free expression, is not unnecessarily burdensome on the conduct of legitimate business, and provides clarity and predictability for businesses operating via the Internet.